INDEX

Abene, Mark (Phiber Optik), 70
Access key, 72
AccessData, 40. *See also* FTK
ActiveX, 77
ADC (analog-to-digital conversion), 21
Adleman, Len, 51
Admissibility of evidence
  acceptable alteration of evidence, 29
  chain of custody, 119, 134, 135
  and choosing course of action, 29, 30
  and goal of computer forensics, 13
  hearsay, 135–137
  and record keeping, 53
  relevance, 132–134
  reliability, 26, 131, 132, 135, 136
Adware, 75, 77, 78
American Standard Code for Information Exchange (ASCII), 18, 39
Analog-to-digital conversion (ADC or A/D), 21
Analog versus digital, 17, 18, 21
Analysis
  application and file analysis, 123, 124
  data encryption, 47–49
  deleted files, 43, 44
  execution files, 41
  file extensions, 44, 45
file slack. *See* File slack
  file structures, 45, 46
  hidden data, 123
  password cracking, 49, 50
  record keeping, 40
  searches, 39, 41
  steganography, 46, 47
  time and date stamps, 41–43, 115, 122, 124
  time frame, 122
  tools for, 39, 40
Answers, 60
Antivirus software, 78, 79
Appearance points (AP), wireless networks, 73, 74
Appendixes, inclusion in report, 56
Apple Computer, 6
Application and file analysis, 123–125
Application suites, 39, 40, 55
ARPANET, 4
Arrest and arraignment, 60
ASCII (American Standard Code for Information Exchange), 18, 39
Assembly language, 3
Asymmetric keys, 48, 49
ATA disks, 118
Attorney-client privilege, 61
Auction fraud, 97–99
Authentication, wireless networks, 72
AvantStar Products, 124

Backdoors, 77–79, 112
Backus, John, 3
Bait-and-switch fraud, 98, 99
Base-2, 19
Base-10, 19, 20
Base-16, 19
Basic input output system. *See* BIOS
Basic integrated operating system. *See* BIOS
Best evidence rule, 26, 135
Binary system, 17, 18, 20–22
BIOS, 32, 33, 116, 123
Bit-stream images, 119
Blankenship, Loyd, 8
Booting up
  automatic processes, 122
  BIOS, 32, 33
  and collection of evidence, 31–33
  controlled, 116, 117
  and operating systems, 22, 23
  and preservation of evidence, 27, 28
Bug, computer, 3, 77
Bulletin board systems (BBSs), 7

COPYRIGHTED MATERIAL

Burden of proof, 58
Business records exception to hearsay rule, 136, 137
Bytes and memory blocks, 42, 43

C, 6
C+, 3
C++, 3, 6
Cache files, 114, 124, 125
Card skimming, 90, 91
Carnivore software (FBI), 80, 141, 142
Carving, 121, 122
CD (compact disc) as storage unit, 16
Cellular phones as storage unit, 16
Central processing unit (CPU), 15, 17
Chain of custody, 119, 134, 135
Chat rooms, 95, 96, 101, 102
Child endangerment, 94, 96
Child pornography cases, 41, 94–97, 114
Circumstantial evidence, 128, 129
Civil litigation, 58–63
Clusters, 45, 46, 121
COBOL, 3
Code, 22
Collection of evidence
  procedure, 31–37
  record keeping, 30
Color, 20, 21
Compact disc (CD) as storage unit, 16
Complaints, 59
Computer crimes, 66, 88, 89. *See also* Criminal liability
  auction fraud, 97–99
  child pornography and child endangerment, 94–97
  counterfeiting, 100
  cyberstalking, 102
  forgery, 100
  identity theft, 89–94
  online retail fraud, 99
  piracy, 103–105
  prostitution, 100, 101
  securities fraud, 101, 102
Computer data described, 17–23
Computer Fraud and Abuse Act, 76
Computer literacy, 70
Computers
  basic operation of, 14–24
  historical background, 3–5
  ubiquitous nature of, 14
Conclusion of report, 56
Control/Program Monitor (CP/M), 6
Copying
  and file slack, 34, 35, 42, 43
  imagers. *See* Imagers
  importance of copying data drive, 42
  software, 84
Copyright infringement, 104
Corporate espionage, 79, 80, 82
Counterfeiting, 89, 100
CPU (central processing unit), 15, 17
Credit cards, forgery and fraud, 90–92
Criminal liability. *See also* Computer crimes
  arrest and arraignment, 60
  burden of proof, 58
  civil litigation distinguished, 58
  expert witnesses, use of, 61
  historical background, 9, 10
  information or indictment, 59
  offense as start of case, 58
  penalties, 60
  plea agreements, 62
  trials, 62, 63
Cross-examination, 135, 136
Cryptanalysis, 82, 83, 123
Cryptography, 46, 80. *See also* Encryption
Cult of the Dead Cow, 68
Curricula vitae (CV), investigator's, 56
Cyberstalking, 102
Cyberterrorists, 70, 71, 85

Data retrieval from dead system, 116–118, 120–122
Daubert v. Merrill Dow Pharmaceuticals, 64, 131, 132
Defendants, 59
Defragmentation, 44
Deleted files, 43, 44, 121, 122
Demon Dialer, 68
Demonstrative evidence, 129
Department of Defense (DOD)
  and growth of Internet, 4
  vulnerabilities, 70, 71
Depositions, 60–62
Diagnostic software, 123
Digital evidence, 1
  collection of, 13

historical background, 10
nature of, 14, 15
preservation of, 13, 14
Digital fingerprinting, 113
Digital Intelligence, 120
Digital Signal Line (DSL), 6
Digital versus analog, 17, 18, 21
Digital video disc (DVD) as storage unit, 16
Direct evidence, 128, 129
Discovery, 60–62
investigator's qualifications, 56
production orders, 109
Disk architecture, 34
Disk drives, removal of, 31
Disk failure, 45
Disk fragmentation, 44
Disk imaging software, 33, 34
Disk Operating System (DOS), 6
Disk-write blocking programs, 33
.dll files, 111, 112
Documentary evidence, 129
Documentation. *See also* Record keeping; Reports
photographs, 53, 54
supporting documents, inclusion in report, 56
Draper, John (Captain Crunch), 68
Drive slack, 34
DriveSpy, 117
DSL (Digital Signal Line), 7
Dumpster diving, 80, 89, 90
DVD (digital video disc) as storage unit, 16
Dying declarations, 136
Dynamic linked library (.dll) files, 111, 112

E-mail
analysis tools, 40
anonymous, 96, 99
and cyberstalking, 102
and cyberterrorists, 70
and phishing, 93
and Trojan horses, 76, 77
wiretaps, 80, 81, 139, 140
eBay, 97
802.11 standard, 72, 73
Electronic Communications Privacy Act (ECPA), 140
Email Examiner, 40
Embedded systems, 16
Employees
consumer information, misuse of, 94
disgruntled, 80, 82
monitoring, 142
theft, 83–85
Encase, 40, 43, 55, 111, 112, 117, 121
Encrypted File System (EFS), 114
Encryption, 47–49
and file ransom, 80
and system memory searches, 114
and wireless networks, 72, 73
Engressia, Joe, 67
Eudora, 81
Evaluation of case, 109, 110
Evidence
admissibility. *See* Admissibility of evidence
best evidence rule, 26, 135
circumstantial, 128, 129
collection of, 30–37
destructive testing, 28, 29
direct, 128
evaluation of, 110–115
preservation of, 26–30
reliability, 26, 131, 132, 135, 136
types of, 129, 130
Excited utterance exception to hearsay rule, 136
Execution files, 41
Executive summary, 55
Expert witnesses
communication skills, 64, 65
Daubert factors, 64, 131, 132
depositions, 61, 62
lay witnesses distinguished, 130
opinion testimony, 63, 64, 130
qualifications, 61, 64
roles of, 62–65
testimony, 61, 63–64, 130–132
Exploits, 7

Federal Bureau of Investigation (FBI), Carnivore software, 80, 141, 142
Federal Rules of Evidence
investigator's curricula vitae, 56
scientific evidence, admissibility of, 132
Federal Trade Commission (FTC), identity theft complaints, 89
Fermi, Enrico, 4

File extensions, 44, 45
File formats, graphic images, 21
File names, 125
File ransom, 80
File slack, 30, 34, 35, 42, 43
File structure, 45
File system rootkit, 111
File Transfer Protocol (FTP), 105
Findings, 55
Flash drives, 15
Flash memory disk, 120
Florida Department of Law Enforcement, 97
Foremost, 122
Forensic Accounting and Fraud Investigation for Non-Experts, 64
Forensic boot floppy, 116, 117
Forensic Recovery of Evidence Device (F.R.E.D.), 120
Forensic science defined, 2
Forensic Toolkit, 40
Forensic workstation, portable, 120
Forgery, 89, 91, 100
FORTRAN, 3, 22
Fourth Amendment. *See* Search and seizure
Fragmented files, 122
F.R.E.D., 120
Frye test, 131
FTK, 40, 55, 121, 122

Gates, Bill, 4, 5
Geometry of disk, 35, 118
Gigabyte (GB), 16, 36
Global positioning system (GPS) and war driving, 72
Goal of computer forensics, 2, 10, 13
Goggans, Chris (Erik Bloodaxe), 70
GPU (graphics processing unit), 15
Graphic processing card, 21
Graphical user interface (GUI), 5, 6
Graphics files, 46
Graphics processing unit (GPU), 15
Great Hacker War, 8
GUI (graphical user interface), 5, 6
Guidance Software, 40

Hacker Defender, 112
Hacker Manifesto, 7, 8, 67
Hackers
  black hat, 69, 70
  computer literacy, 70
  and corporate espionage, 83
  cyberterrorists, 70, 71
  gray hat, 69
  hactivists, 70
  historical background, 6–10, 67, 68
  insiders, 82
  mainframes, use of, 82, 83
  origin of term, 67
  phishing, 92, 93
  potential for harm, 70, 71
  script kiddies, 69, 70
  white hat, 69
  wireless hacking, 71–75
Hacker's Quarterly, The, 68
Hactivists, 70
Harassment. *See* Cyberstalking
Hard drives
  architecture, 123
  disconnecting, 116
  imaging, 118–120
  partitions, 37, 41, 45, 82, 116, 121, 123, 124
  as storage unit, 16
  timeframe for searching, 39
Hardware incompatibility, 36
Hardware write blocker, 33, 117, 118
Hashing, 113, 114
  and chain of custody, 119, 134, 135
  hard drive prior to imaging, 118–120
Hearsay, 135–137
Hertz, 21
Hex Workshop, 117
Hexadecimal notation (hex), 18–20, 39, 44
Hidden data analysis, 123
Hidden partitions, 121, 123
History of computer forensics, 2–5
Hooking, 112
Host protected area (HPA), 123
HTML (hypertext markup language), 5, 6

IBM and history of computers, 3, 4
Identity theft, 89–96, 99
Imagers, 33, 34, 38, 40, 50, 51, 118–120
Impeachment, 61
Indictment and information, 59
Input devices, 15
Interception of communications, 140, 141
Internet

and child pornography. *See* Child pornography cases
and development of HTML, 5, 6
history, 124, 125
origin of, 4, 5
Internet Explorer, 77, 80, 93
Internet Protocol (IP) address, 99, 115
Internet Relay Chat (IRC), 104, 105
Interrogatories, 60
Intrusion detection, 6, 9–11
iPods as storage unit, 16

Java, 77, 80, 81
Jobs, Steve, 4, 5
Jury selection, role of expert, 62

Kernel-mode rootkits, 112
Key word searches, 41
and data extraction, 121
and imaging devices, 119, 120
Keyboards, 15, 54
Keystroke monitoring, 78, 80, 142
Kilobyte (KB), 32
Kumho Tire Co. v. Carmichael, 132

Laptops
security issues, 84
and wireless networks, 71–75
Law enforcement
and case evaluation, 109
and computer crime, 9, 10
interagency cooperation, 99
searches and seizures, 137–139
Lebed, Jonathan, 102
Legion of Doom, 8, 68, 70
Library rootkits, 111, 112
Linux, 22, 32
Local area network (LAN), 71, 74
Logical disks, 32, 37
Logical drives, 45
Logicube, 120
Login attempts, 115
Logistical issues, 109, 110

Machine language, 3
Magnetic stripe encoder, 91
Mainframe computers, 82
Malware, 74–79, 85
Marconi, Guglielmo, 4
Masters of Deception, 8, 68, 70
MD5, 120
Megabyte (MB), 16
Memory blocks, 42–44
Mentor, The, 8
Metadata, 123
Microsoft Encrypted File System (EFS), 114
MILnet, 4
Money, 49
Monitors, 15, 21, 23
Morris, Robert Tappan, 76
Morris worm, 76
Motherboard, 33
Motions, pretrial, 60
Mouse
as input device, 15
keystroke monitoring, 142
and preservation of evidence, 28, 30, 54
MOVE, 3
Mozilla, 114
MP3 players, 16, 21
Mpeg-4, 21
Music files, 21, 103–105
My Key Technologies, 123
MyKey DriveCopy, 120

Napster, 104
National Security Agency (NSA), 70
Network information, 115
Norton Disk Editor, 117
Norton Utilities, 43, 121

Objections, depositions, 62
Ogg-Vorbis, 21
On-site capture of evidence, 31, 32, 54, 110
Online auctions. *See* Auction fraud
Online retail fraud, 99
Opening statements, 63
Operating systems (OS)
access level, 82
and BIOS, 32. *See also* BIOS
and collection of evidence, 31
computer programs distinguished, 22, 23
controlled boot, 116, 117
CP/M, 6
DOS, 6
dual-boot systems, 124
and file structure, 45, 46

Operating systems (OS) (*continued*)
MS-DOS 6.22, 117
and preservation of evidence, 27, 28
as programs, 22
Windows, 17, 112
Outlook, 81
Output devices, 15, 23
Ownership analysis, 125

Packet sniffers, 77
Paraben Software, 40
Partitions, 37, 41, 45, 82, 116, 121, 123, 124
Passwords
brute-force attack, 49, 82, 83
cracking, 40, 82, 123
and data extraction, 121
file slack, searching, 43
and identity theft, 93
and keystroke monitors, 80
and ownership analysis, 125
protection systems, 49
reuse of, 50, 114, 123
and social engineering, 50
and spyware, 78
and steganography, 47
and system memory, 114
and Trojan horses, 77
wireless networks, 72
Patterns, 124
Peer-to-peer (P2P) file sharing, 104, 105
Pen tablets as input devices, 15
Permissions, 81, 82, 84
Personal computers (PCs), 3, 4
PGP (Pretty Good Protection), 47, 48
Phishing, 92, 93
Photographs
digital storage, 18, 20
as documentation, 53, 54
and hashing, 113
Phreakers, 67–69
Physical disks, 32, 37
Piggybacking, 75
Piracy, 103–105
Pixels, 21
Plaintiffs, 59
Plea agreements, 62
Point of sale (POS), 90
POP, 3
POST (power-on self-test), 32
Preservation of evidence
course of action, choosing, 29, 30
importance of, 26, 27
keyboard, use of, 54
mouse, use of, 28, 30, 54
and online transactions, 99
problems with, 27, 28
record keeping, 27, 29
testing and other alteration of evidence, 28, 29, 110, 111
Pretrial, 60, 61
Pretty Good Protection (PGP), 47, 48
Printers, 15, 23
Private key, 48, 49
Process tables, 114
Processing unit, 15–23
ProDiscover, 111, 112
Programming languages, 3, 6, 22
Proprietary technology, 14, 21
Prostitution, 100, 101
Public key, 48, 49
PUSH, 3

Quick View Plus, 124
QuickBooks, 49

RAID, 36, 110, 116
RAM (random access memory), 15
and collection of evidence, 31
printers, 23
slack, 30, 42, 43
as storage unit, 16
Ransom, 80
Real evidence, 129, 135
Record keeping
and application suites, 40
collection of evidence, 30
and evaluation of evidence, 110
on-scene documentation, 53–55
and preservation of evidence, 27, 29
system components, 116
Redundant array of inexpensive disks. *See* RAID
Relevance, 132–134
Reliability of evidence, 26, 135–137
expert testimony. *See* Expert witnesses
scientific evidence. *See* Scientific evidence

Reports
and application suites, 55
discovery issues, 61
importance of, 53
photographic documentation, 53, 54
presentation, 57
sections of, 55, 56
uses of, 57
RGB color system, 20, 21
Rivest, Ron, 51
Root-level access, 82
Rootkits, 78, 79, 82, 111, 112, 115
Routing tables, 114, 115
RSA encryption, 49, 51
Running processes, 115

S-Tools, 124
Sabotage, 80
SafeBack, 117
Sanderson Forensics, 123
Scalpel, 122
Scanners as input devices, 15
Scarfo, Nicodemo, 142
Scientific evidence, 131, 132. *See also* Expert witnesses
Script kiddies, 69, 70
SCSI disks, 118
Search and seizure, 127, 128
consent, 140, 141
exclusionary rule, 137
Fourth Amendment rights, 137–139
legislation, 139–142
probable cause, 138
warrants, 138, 139, 141
Search warrants, 31, 32, 109, 138, 139, 141
Searches
authorization, 109, 110
key words, 41
Sectors, 45, 123
Securities fraud, 101–105
Security policies and e-mail wiretaps, 81
Serial numbers, hard drive, 118
Service of process, 59, 60
Settlements, 59, 62
Sexual offender databases, 96, 97
Shamir, Adi, 51
Shoulder surfing, 90
Silverstone, Howard, 64
Slack, 30, 34, 35, 42, 43
SnapCopy, 117
Social engineering, 50, 90, 93
Software, installation of and company-issued laptops, 84
Software, theft of, 83
Software incompatibility, 36
Software piracy, 104
Software write blocker, 33
Spyware, 75, 77, 78, 80
Stand-alone tools, 39, 40, 43
Start-up. *See* Booting up
Steganalysis, 123
Steganography, 46, 47, 96, 124
Storage
arrays, 36
devices, 15
Symantec Corporation, 43, 80
System components, 116
System information, alteration of, 28, 29, 110, 111
System memory, 114
System scheduling, 115
Systems administrators
and consent under Electronic Communications Privacy Act, 140, 141
early attitudes toward hackers, 9
user access and permissions, 81, 82, 84
and wireless networks, 73, 74

Table of contents, reports, 55
Technology Pathways, 111, 123
Telephone charges and dial-up modems, 67
Terabytes (TB), 36, 109
Testimony. *See also* Expert witnesses
as evidence, 129
expert versus lay witnesses, 61
Theft, 84, 85
Time and date stamps, 41–43, 115, 122, 124
Time frame analysis, 122
Trade secrets and corporate espionage, 79, 80, 83
Trials
civil, 57, 58, 62–65
criminal, 58, 62–65
phases of, 57
pretrial phase, 60–62
settlements, 59

Trojan horses, 75–77, 80, 81, 84
Trusted entity scams, 91

Universities and development of Internet, 4, 5
UNIX, 6
U.S. v. Scarfo, 142
Usenet newsgroups, 104, 105
User access, 81, 82, 84
User information, 115
Username
  and identity theft, 93
  wireless networks, 72

Video files, illegal copying, 103–105
Virus protection software, 78, 79
Viruses, 75–77, 84
Voir dire, 61
Volatile memory, 114, 115

War chalking, 73
War dialing, 68
War driving, 72
Web browsers, 77
Web sites, phony, 93
Wi-Fi, 72, 84
Windows, 17, 22, 32, 112
WinHex, 20, 39, 121, 122
Wireless networks, hacking, 71–75
Wiretap Act (Title III), 139, 140
Wiretaps, 80, 81, 139, 140
Witnesses
  cross-examination, 135, 136
  expert. *See* Expert witnesses
  lay witnesses, 61, 130, 131
Word processing, 18
World Wide Web, development of, 5, 6
Worms, 75–77, 84
Wozniak, Steve, 4, 5
Write blocking, 33, 38, 117, 120, 122

X-Ways Software, 39